AMENDMENTS TO THE CLAIMS

1. (Previously Presented) A method, comprising:

receiving a request for hardware component information at a service processor disposed in a hardware component as an open session request from a requesting client application;

transmitting from the service processor a challenge string to the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

receiving at the service processor a challenge response from the requesting client application, the challenge response including the session identification;

comparing the challenge response to an expected response to the challenge string, wherein the comparing includes verifying the session identification received in the challenge response against the session identification transmitted in the challenge string; and

transmitting the hardware component information to the requesting client application.

Claims 2-3 (Cancelled)

4. (Previously Presented) The method according to claim 1, wherein the challenge response includes a sequence number that increments with every new message.

5. (Canceled)

6. (Previously Presented) The method according to claim 1, further comprising examining each packet received from the client application for one or more of the following: the session identification, the sequence number, and a hash number.

7. (Previously Presented) The method according to claim 6, wherein the hash number comprises a function of one or more of the following: the session identification, the sequence number, and a packet.

8. (Previously Presented) A method, comprising:

transmitting a request for hardware component information to a service processor disposed in a hardware component as an open session request from a requesting client application;

receiving from the service processor a challenge string at the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

transmitting to the service processor a challenge response from the requesting client application, the challenge response including the session identification; and

receiving from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated in the service processor, wherein the comparison includes verifying the session identification in the challenge response transmitted to the service processor against the session identification received in the challenge string.

Claims 9-11 (Cancelled)

12. (Previously Presented) The method according to claim 8, further comprising transmitting with each packet sent by the client application one or more of the

following: the session identification, the sequence number and a hash number, wherein the hash number includes a function of one or more of the following: the session identification, the sequence number, and a packet.

13. (Previously Presented) An apparatus, comprising:

a remote access port; and

a service processor coupled to the remote access port, wherein the service processor including a machine-readable medium, having stored thereon a set of instructionswhich, when executed, cause the service processor to:

in response to a remote request for information about a component received as an open session request through the remote access port external to a host operating system of the apparatus, transmit a challenge string to a requesting client application, the challenge string including session identification assigned by the service processor, wherein the session identification is unique to each session;

compare a challenge response received from the requesting client application with an expected response, the challenge response including the session identification, wherein the comparing includes verifying the session identification received in the challenge response against the session identification transmitted in the challenge string; and

transmit an authentication response to the requesting client application based on the comparison.

Claims 14-15 (Cancelled)

16. (Original) The apparatus according to claim 13, wherein the service processor compares a sequence number included in the challenge response against previously received sequence numbers and ignores the challenge response if it does not include a sequence number in correct sequence.

17. (Original) The apparatus according to claim 13, wherein the service processor compares a hash number received in the challenge response with an expected hash calculated by the service processor and transmits a success or failure message depending upon a result of the comparison.

Claims 18-19 (Cancelled)

20. (Previously Presented) A system, comprising:

a processor;

a memory; and

a client application stored on a machine-readable medium, the client application including a set of instructions which, when executed, cause the client application to:

transmit a request for hardware component information to a service processor disposed in a hardware component as an open session request;

receive from the service processor a challenge string at the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

transmit to the service processor a challenge response from the requesting client application, the challenge response including the session identification; and receive from the service processor an authentication response to the requesting client application based on a comparison of the challenge response from the requesting client application and an expected challenge response calculated at the service processor, wherein the comparison includes verifying the session identification received in the challenge response against the session identification in the challenge string.

21-30 (Canceled)

31. (Previously Presented) A machine-readable medium having stored thereon a set of instructions which, when executed by a machine, causes the machine to:

receive a request for hardware component information to a service processor disposed in a hardware component as an open session request;

transmit from the service processor a challenge string at the requesting client application, the challenge string including a session identification assigned by the service processor, wherein the session identification is unique to each session;

receive at the service processor a challenge response from the requesting client application, the challenge response including the session identification;

compare the challenge response to an expected response to the challenge string, wherein the comparing includes verifying the session identification received in the challenge response against the session identification transmitted in the challenge string; and

transmit the hardware component information to the requesting client application.

Claims 32-33 (Cancelled)

34. (Previously Presented) The system according to claim 20, wherein the service processor compares a sequence number included in the challenge response against previously received sequence numbers and ignores the challenge response if it does not include a sequence number in correct sequence.

35. (Previously Presented) The system according to claim 20, wherein the service processor compares a hash number received in the challenge response with an expected hash calculated by the service processor and transmits a success or failure message depending upon a result of the comparison.

36. (Previously Presented) The machine-readable medium according to claim 31, wherein the challenge response includes a sequence number that increments with every new message.

37. (Previously Presented) The machine-readable medium according to claim 31, wherein the set of instructions which, when executed by the machine, further causes the machine to examine each packet received from the client application for one or more of the following: the session identification, the sequence number, and a hash number.